Wireless Pers Commun (2018) 98:2009–2023
https://doi.org/10.1007/s11277-017-4960-2

Secure Audio Cryptosystem Using Hashed Image LSB watermarking and Encryption

Osama S. Faragallah[1,2]

Published online: 25 October 2017

Abstract The paper proposes a secure audio cryptosystem that realize integrity, authentication and confidentiality. The proposed audio cryptosystem achieves integrity by applying a message digest algorithm, authentication by employing LSB watermarking and confidentiality through encryption with Advanced Encryption Standard (AES) or RC6. The main concept of the proposed audio cryptosystem relays on XORing the plain-audio with one selected image from a private image database. Then, the mixed plain-audio blocks are LSB watermarked with the selected image hash value prior to ciphering. The proposed audio cryptosystem is prepared with the potential of increasing immunity against brute force attacks and providing integrity, authentication and confidentiality through the selected image hash value addition using LSB embedding as an extra key. Also, the extra XORing step removes residual intelligibility from the plain-audio blocks, fills the speechless intervals of audio conversation and helps in destroying format and pitch information. The proposed audio cryptosystem is compared with audio encryption using AES, and RC6 through encryption key performance indicators. The comparison outcomes ensured the superiority of the proposed audio cryptosystem. Security investigation of the proposed audio cryptosystem is studied from a precise cryptographic standpoint and tests ensured the superiority of the proposed audio cryptosystem from a cryptographic standpoint.

Keywords AES · RC6 · Brute force attacks · Diffusion

✉ Osama S. Faragallah
osam_sal@yahoo.com; o.salah@tu.edu.sa

[1] Department of Computer Science & Engineering, Faculty of Electronic Engineering, Menoufia University, Menouf 32952, Egypt

[2] Department of Information Technology, College of Computers and Information Technology, Taif University, P.O. Box 888, Al-Hawiya 21974, Saudi Arabia

1 Introduction

Confident audio telecommunications are commonly utilized in the corporate, military branches and Internet. Generally, any telecommunication arrangement like wireless systems may not give adequate security with attacks and eavesdroppers throughout communication. If the transferred audio files are plain or not ciphered, the transferred plain audio files may be subjected to any unauthorized eavesdropper. Internet itself does not guarantee adequate security estimations, and there is no guarantee that the transferred plain-audio over it can not be intercepted in between [1]. To ensure a traffic security high level, end-to-end ciphering and authentication are required [2]. It is so significant to safeguard audio calls through wire and wireless telecommunications with efficient and secure audio cryptosystems.

The paper presents an efficient audio cryptosystem approach that is capable of providing integrity, authentication and confidentiality for audio streams telecommunication. This is achieved by using message digest algorithm, LSB watermarking and encryption. The LSB watermarking of the selected image hash value (message digest) in the private image database is utilized to guarantee and ensure the correct speaker identification. At the destination, a deciphering procedure followed by watermark extraction is carried out as a test for an authorized speaker. The paper rest include the following sections. Section 2 overviews the utilized tools with the proposed audio cryptosystem like AES, RC6 and the MD5 algorithm. Section 3 presents the proposed audio cryptosystem. Section 4 gives test results. Lastly, conclusions are explored in Sect. 5.

2 Utilized Tools

2.1 AES

AES is commonly utilized in banking and telecommunication. This is because of its suitability for hardware implementation in which soft cost and power consuming were required in addition to its strong security and efficient processing time [3, 4].

AES may be considered as a private symmetric iterative block cipher that allows a changeable block size, a changeable secret key size, and a changeable number of rounds. The AES allows 128, 192 or 256 bits for both block size and secret key size. The rounds number carried out is influenced by secret key size. The number of rounds is 10, 12, and 14 for 128, 192 or 256 bits secret key size, respectively. The resulted cipher is known as state and consists from square matrix of four rows and columns corresponds to block size split by 32. The secret key is also square matrix of four rows and columns corresponds to secret key size split by 32.

Every round combines original plain information with round secret key that computed using ciphering key. The deciphering process reverses iterations producing a fractionally different data path. The AES cipher preserves an internal matrix of 4 by 4 bytes, known as state, on which procedures are employed. The initial state contains original input plain information block that XORed with cipher secret key. Normal rounds include procedures known as Add Round Key, Mix Columns, Shift Rows, and Sub Bytes. The final round excludes Mix Columns. The Sub Bytes is a reversible nonlinear conversion. It utilizes 16 similar 256-byte S-box to map every state byte into a different byte. The S-box inputs are produced through estimating multiplicative reverses within Galois Field GF (2^8) and performing affine transformations. The Sub Bytes may be achieved either by substitution estimation [5, 6] or using look up tables [7, 8]. The Shift Rows is a periodical state left shift by one, two, and three bytes of second, third, and fourth row, respectively. The Mix Columns employs modular polynomial multiplication within GF (2^8) on every column. The Sub Bytes and Mix Columns can be mixed into extensive look up tables known as T-boxes [9]. Through every round, Add-Round-Key employs XOR with state and round key.

2.2 The RC6 Cipher

The RC6 can be considered as confusion/diffusion based block cipher. It is commonly utilized for data ciphering and may be adjusted for multimedia encryption. The RC6 cipher utilizes four running registers and each register size is 32 bit. So, it can operate on 128 bit input/output blocks. The RC6 cipher is composed from two Feistel networks for mixing data using rotations. The procedures for each round of the RC6 cipher are two applications of the squaring function $y(x) = x\ (2x + 1) \bmod 2^{32}$, two fixed 32-bits rotations, two 32-bits data-dependent rotations, two XORs, and two modulo 2^{32} additions. The RC6 cipher can be precisely specified as RC6-w/r/b, where w represents the word size in bits, r represents the number of rounds, and b represents the encryption key length in bytes. The utilization of multiplications in RC6 extremely enhances the obtained diffusion per round, granting high security, few rounds, and an improvement in the performance [10–14]. Unlike many ciphers, the RC6 does not utilize look up tables through encryption/decryption. This implies that the RC6 code and data can be adequate for today's on-chip cache memories. The RC6 cipher offers several features like simplicity, compactness, security, superior performance and considerable flexibility [10].

2.3 The MD5 Algorithm

The MD5 is utilized to generate a message digest that is used to provide a fingerprint or message digest for the selected image from the private database. This fingerprint is utilized as a message authentication code (MAC) for the selected image. The MD5 takes as input an image of arbitrary length and generate as output a 128-bit fingerprint or message digest [15, 16]. The MD5 is designed to be quite fast on 32-bit machines. In addition, MD5 does not require any large substitution tables.

3 The Proposed Audio Cryptosystem

The proposed audio cryptosystem is utilized to achieve integrity, authentication and confidentiality. The detailed ciphering procedure of the proposed audio cryptosystem may be listed as:

1. The plain-audio signal is framed and reshaped into 4 × 4 byte blocks.
2. Select an image from the private image database.
3. The selected image is XORed with 4 × 4 byte blocks of the plain-audio signal.
4. The 128-bit selected image hash value is embedded using LSB watermarking into each 8 mixed plain-audio blocks.
5. The outcome plain-audio blocks are ciphered using AES or RC6.

The detailed deciphering procedure of the introduced audio cryptosystem may be listed as:

1. The cipher-audio is framed and reshaped into 4 × 4 byte blocks.
2. The ciphered-audio blocks are decrypted using AES or RC6.
3. Extract the selected image hash value using LSB watermarking extraction phase.
4. Every audio block is XORed with the image which corresponds to the same extracted image hash value.

Figure 1 shows a block diagram for the proposed audio cryptosystem.

3.1 Preprocessing Phase

For the proposed audio cryptosystem, a private database that contains 512 images and their corresponding hash values is prepared. The size of each image and its corresponding hash value is 128 bit. Initially, the user selects a given image, and then each audio block of the plain-audio of 128 bit size is XORed with the selected image. Each outcome mixed audio block is watermarked with the hash value of the selected image using LSB embedding. The hash value of the selected image is 128 bit and it is embedded to each 8 mixed audio blocks. The steps of preprocessing phase are illustrated in Fig. 2. Figure 2a illustrates the mixed plain-audio block after XORing with the selected image. Figure 2b shows the 128-bit hash value of the selected image. Figure 2c shows the least significant bits of sixteen bytes of the mixed plain-audio block after XORed with the selected image that will

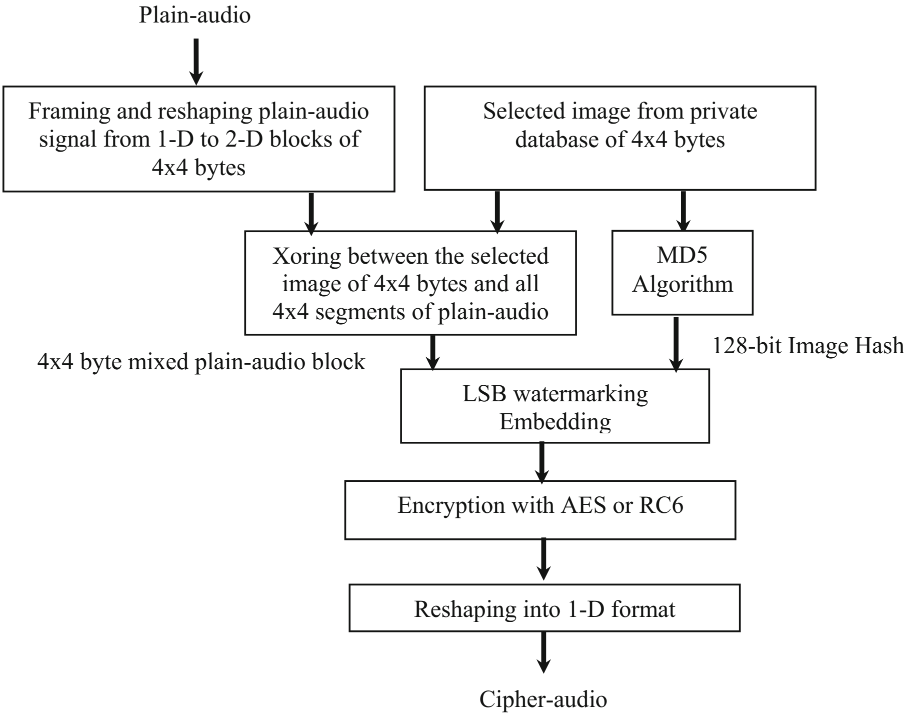

Plain-audio
Framing and reshaping plain-audio signal from 1-D to 2-D blocks of 4x4 bytes
Selected image from private database of 4x4 bytes
Xoring between the selected image of 4x4 bytes and all 4x4 segments of plain-audio
MD5 Algorithm
4x4 byte mixed plain-audio block
128-bit Image Hash
LSB watermarking Embedding
Encryption with AES or RC6
Reshaping into 1-D format
Cipher-audio

Fig. 1 Block diagram of the proposed audio cryptosystem

Fig. 2 The steps of preprocessing phase for XORing the 4 × 4 byte plain-audio block with the selected image from private image database and embedding the 128 bit selected image hash value using LSB watermarking to each 8 mixed audio blocks. **a** 4 × 4 byte mixed plain-audio block after XORing with the selected image. **b** The 128-bit hash value of the selected image. **c** The least significant bits of sixteen bytes of the mixed plain-audio block after XORed with the selected image. **d** The output audio block after embedding the first 2 red marked bytes of the selected image hash value

11001110	10010111	10101001	11010010
10011111	0001101	10000011	11100011
11110001	11001011	00001101	10010011
10100110	10110010	11100111	10111011

(a)

11011011	01101111	11011111	00001111
10001110	10001110	11011111	00001101
10101110	10110110	11010111	10000111
01110001	01100110	11010010	11001010

(b)

1100111X	1001011X	1010100X	1101001X
1001111X	000110X	1000001X	1110001X
1111000X	1100101X	0000110X	1001001X
1010011X	1011001X	1110011X	1011101X

(c)

11001111	10010111	10101000	11010011
10011111	0001100	10000011	11100011
11110000	11001011	00001101	10010010
10100111	10110011	11100111	10111011

(d)

be replaced by the first 2 red marked bytes of the selected image hash value. Note that the 128 bit selected image hash value is embedded to each 8 mixed audio blocks using LSB watermarking. Figure 2d shows the output audio block after embedding the selected image hash value.

As seen from Fig. 2d, the change amount for each audio block may be rated as insignificant and cannot affect the audio quality. The output audio blocks contain the selected image hash value that is embedded with the mixed plain-audio blocks using LSB watermarking.

3.2 Encryption

Now, each audio block resulted from the preprocessing phase is subjected to encryption phase using AES or RC6. Now, the resulted ciphered-audio blocks are firstly masked with selected image, then LSB watermarked with the selected image hash value and finally encrypted with AES or RC6.

4 Experimental Tests

In this part, we know in advance that AES and RC6 are known as secure and efficient encryption algorithm. So, we are fundamentally interested with investigating the impact of quality enhancement presented by LSB watermarking of the selected image hash value in the mixed plain-audio blocks as a preprocessing step prior to encryption. Also, we are interested with studying the effect of quality degradation introduced in the decrypted ciphered audio. This section is divided into two subsections; one for investigating the quality of the ciphered audio and the other for investigating the quality of the deciphered audio. Simulation tests were employed in MATLAB R2013a with windows7 environment. All tests were implemented using the Handel signal available in Matlab as shown in Fig. 3a with an audio segment of 65,536 samples used as plain-audio signal.

4.1 Ciphered-Audio Quality

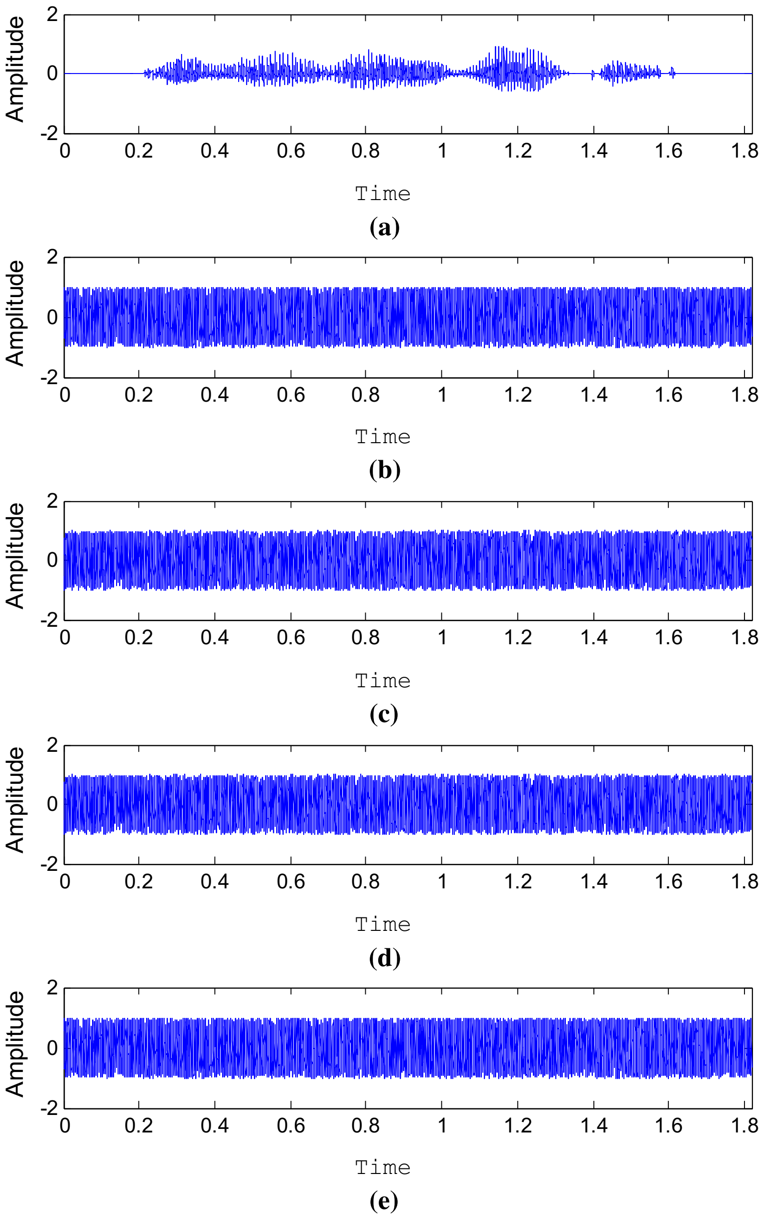
The ciphered-audio is tested to prove and ensure quality enhancements introduced through addition of LSB watermarking preprocessing stage prior to encryption. The proposed audio cryptosystem security is inspected against several attacks like statistical, brute-force, and differential attacks [17, 18]. The test results ensured and verified the superiority of proposed audio cryptosystem from a cryptographic standpoint.

4.1.1 Residual Intelligibility

The Handel plain-audio signal shown in Fig. 3a is encrypted only with the AES and RC6 without LSB watermarking, and outcomes are illustrated in Fig. 3b and c. The exact Handel plain-audio signal is applied to the proposed audio cryptosystem with AES and RC6, and outcomes are illustrated in Fig. 3d and e. Figure 4 shows the Handel plain-audio spectrogram, Handel cipher-audio spectrogram using AES and RC6, and Handel cipher-audio spectrogram using the proposed audio cryptosystem with AES and RC6. It is clear that the cipher-audio appears like random noise with no any audio streams. The plain-audio tones are eliminated, and this guarantees that no residual intelligibility may be valuable for attackers within communication channel.

4.1.2 Statistical Tests

Statistical tests have been examined with the introduced audio cryptosystem for showing its efficient diffusion/confusion features that strongly withstand statistical attacks. Statistical tests include the correlation coefficient of cipher-audio with respect to plain-audio and spectral distortion (SD) of cipher-audio signal compared with plain-audio.



(a)

(b)

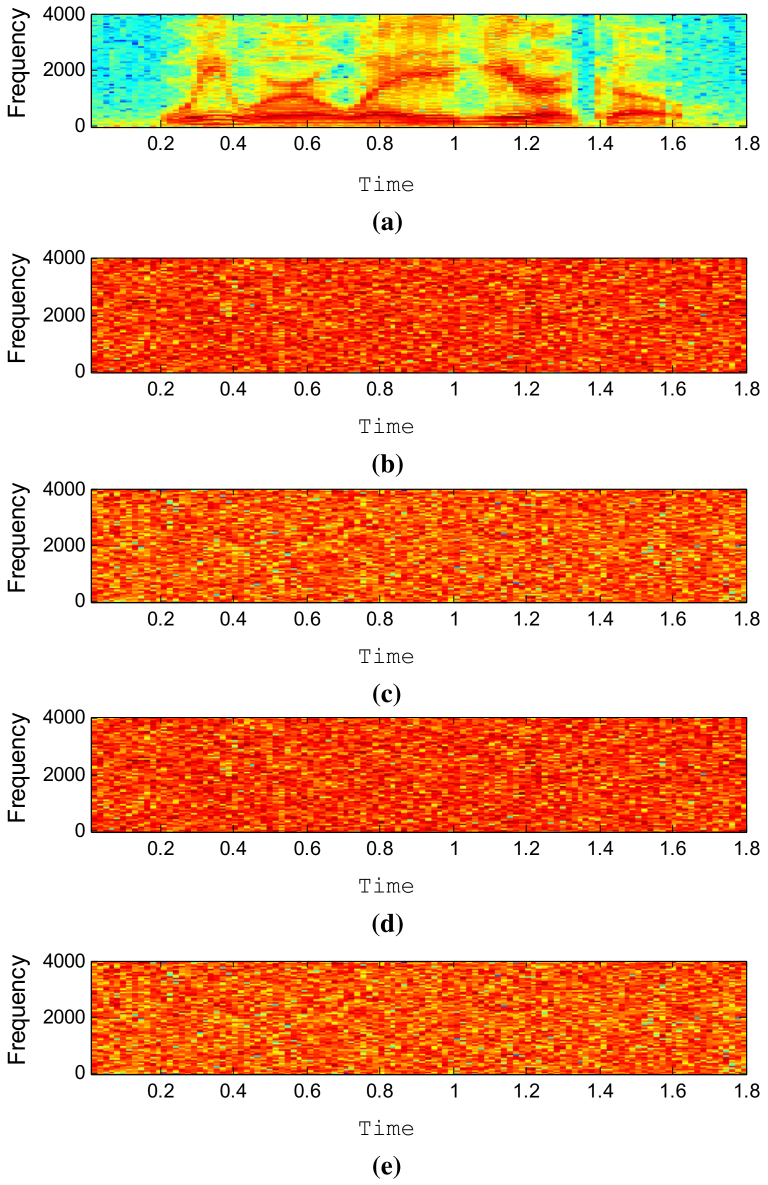
(c)

(d)

(e)

Fig. 3 Encryption results of Handel plain-audio signal. **a** Original Handel plain-audio signal. **b** Handel cipher-audio signal using AES. **c** Handel cipher-audio signal using RC6. **d** Handel cipher-audio signal using the proposed audio cryptosystem with AES. **e** Handel cipher-audio signal using the proposed audio cryptosystem with RC6

4.1.2.1 Correlation Coefficient Metric The correlation coefficient estimation between the plain-audio blocks and its corresponding cipher-audio blocks may be considered as a good estimation to evaluate the encryption quality of the proposed audio cryptosystem. It can be computed as:



(a)

(b)

(c)

(d)

(e)

Fig. 4 Spectrogram results of encrypted Handel plain-audio signal. **a** Original Handel plain-audio signal spectrogram. **b** Handel cipher-audio signal spectrogram using AES. **c** Handel cipher-audio signal spectrogram using RC6. **d** Handel cipher-audio signal spectrogram using the proposed audio cryptosystem with AES. **e** Handel cipher-audio signal spectrogram using the proposed audio cryptosystem with RC6

$$r_{gf} = \frac{\mathrm{cov_v}(\mathrm{g}, \mathrm{f})}{\sqrt{D(g)}\sqrt{D(f)}} \tag{1}$$

where cov$_v$(g,f) represents the covariance among the plain-audio g and the cipher-audio f. *D(g)* and *D(f)* represent the variance of plain-audio g and cipher-audio f. With numerical estimations, the following formulas are employed [19, 20]:

$$E(g) = \frac{1}{N_s}\sum_{i=1}^{N_s} g(i) \tag{2}$$

$$D(g) = \frac{1}{N_s}\sum_{i=1}^{N_s} (g(i) - E(g))^2 \tag{3}$$

$$\mathrm{cov}_v(g,f) = \frac{1}{N_s}\sum_{i=1}^{N_s} (g(i) - E(g))(f(i) - E(f)) \tag{4}$$

where N_s represents the number of audio samples utilized with calculations. Small correlation coefficients r_{gf} value signalizes a perfect encryption quality. The correlation coefficients of the plain-audio and cipher-audio signals using AES, RC6, and the proposed audio cryptosystem with AES and RC6 are given in Table 1.

4.1.2.2 SD Metric The SD is calculated in transform domain on plain-audio frequency spectra and cipher-audio frequency spectra. The SD indicates how far the cipher-audio spectrum from that of plain-audio is.

The SD is computed as [21]:

$$SD = \frac{1}{M}\sum_{m=0}^{M-1}\sum_{i=Nm}^{Nm+N-1} |S_a(i) - S_b(i)| \tag{5}$$

where $S_a(i)$, $S_b(i)$ represent the plain-audio and cipher-audio spectrums in dB for a given block in time domain. The N and M define the block size and the blocks number in the audio. The SD outcomes of the plain-audio and cipher-audio signals using AES, RC6, and the proposed audio cryptosystem with AES and RC6 are given in Table 2.

The obtained results illustrated in Tables 1, 2 ensure that XORing the plain-audio with a selected image and LSB watermarking with the selected image hash value before encryption improve the encryption quality and increase the SD between the plain-audio and cipher-audio signals.

4.1.3 Key Space Test

To obtain a perfect security, the audio cryptosystem must be susceptible to tiny changes in encryption/decryption keys. So, the range of key space must be considerable sufficient to

Table 1 Estimated Correlation coefficients using AES, RC6, and the proposed audio cryptosystem with AES and RC6

Encryption method	Correlation coefficient
AES	0.0075
RC6	0.0079
Proposed audio cryptosystem with AES	0.0042
Proposed audio cryptosystem with RC6	0.0046

Table 2 The SD of the plain-audio and cipher-audio using AES, RC6, and the proposed audio cryptosystem with AES and RC6

Encryption method	SD
AES	28.4877
RC6	26.5862
Proposed audio cryptosystem with AES	34.8224
Proposed audio cryptosystem with RC6	32.4753

withstand and resist against brute force attack. For a secret key of k bits size, the exhaustive key for an opponent examining all possible keys will require 2^k trials to pass. If the secret key size is 256 bits for AES cipher, the attacker will require 2^{256} trials for guessing the secret key. Assume that the attacker utilizes 3000 MIPS to determine secret key, then computational time will demand:

$$\frac{2^{256}}{365 \times 24 \times 60 \times 60 \times 3000 \times 10^6} > 1.223 \times 10^{60} \text{ Years}$$

For the proposed audio security communication system, we have combined additional 128 bits for the embedded selected image hash value, so computational time will be:

$$\frac{2^{384}}{365 \times 24 \times 60 \times 60 \times 1000 \times 10^6} > 4.16 \times 10^{98} \text{ Years}$$

The above estimated computational time is calculated under the condition of recognized secret key size. However, the secret key size must be obscure so the computational time needs will be augmented very much and will be unattainable.

4.1.4 Differential Tests

An eligible feature for perfect audio encryption/decryption is the critical sensibility to slight modifications within input plain-audio signal (like one bit modification in the input plain-audio). Normally, the attacker may perform a small change, like changing just only single bit of the plain-audio signal, and monitoring the result variation. With such method, the attacker can determine a considerable relation among input original audio and output ciphered audio. When a slight modification within input original audio causes a considerable modification within the ciphered audio, the differential attack will be ineffectual and in practice worthless.

With respect to the proposed audio cryptosystem, the sensitivity to a slight change will be inspected by altering just single bit value of the selected image that XORed with the plain-audio and monitoring the output of the audio cryptosystem. To examine the impact of single bit change of the selected image on the entire cipher-audio signal, we utilize four known estimations. The number of pixels change rate (NPCR), the unified average changing intensity (UACI), correlation coefficient r_{gf} and the SD. If we have two ciphered audio signals, whose correspondent selected images have just a single bit inequality, are represented as F1 and F2. Name the bit with grid (x, y) in F1 and F2 as F1(x, y) and F2(x, y), respectively. A bipolar array (S) is defined of identical size like F1 and F2. So, S(x, y) is evaluated using F1(x, y) and F2(x, y). If F1(x, y) = F2(x, y), then S(x, y) = 1; else, S(x, y) = 0. The NPCR can be computed as [22, 23]:

$$\mathrm{NPCR} = \frac{\sum_{i,j} S(x,y)}{MN} \times 100\% \tag{6}$$

where M and N define the height and width of F1 and F2. The NPCR estimates the ratio of the varied pixels number with respect to whole pixels number in F1 and F2.

The UACI can be computed as [22, 23]:

$$\mathrm{UACI} = \frac{1}{MN}\left[\sum_{x,y} \frac{F1(x,y) - F2(x,y)}{255}\right] \times 100\% \tag{7}$$

It estimates the average intensity of variations between F1 and F2. The achieved outcomes are given in Table 3. Small correlation estimations, high SD, high NPCR and high UACI ensured the high sensitivity of the proposed audio cryptosystem to a slight modification in the selected image or input plain-audio signal.

The obtained results given in Table 3 ensured that there is no correlation occurs between the cipher-audio signals although they have been ciphered by the same secret key. This merit depends on the fact that the AES and RC6 ciphers have an efficient and powerful diffusion mechanism.

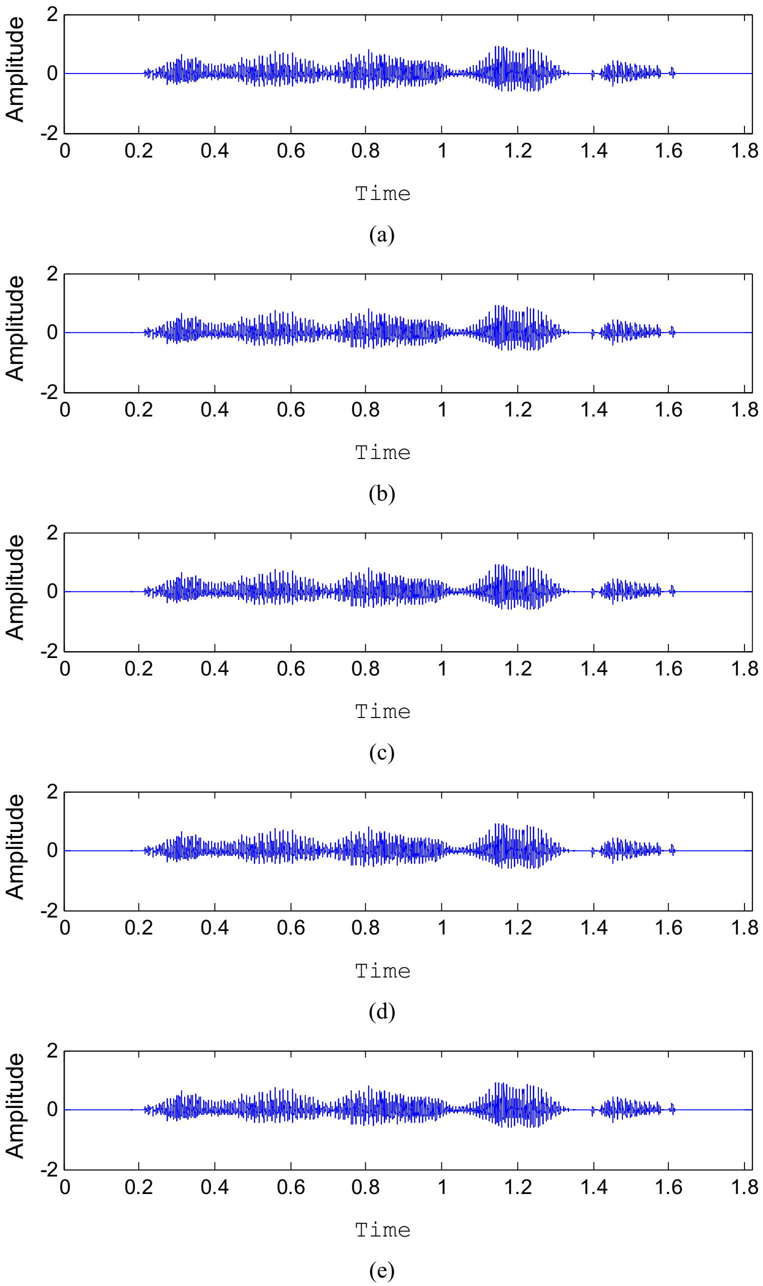
4.2 Deciphered-Audio Quality

The Handel plain-audio signal is ciphered four times using RC6, AES and the proposed audio cryptosystem with RC6 and AES. The cipher-audio signal is deciphered using RC6 and AES, and the decryption results are depicted in Fig. 5b and c. The cipher-audio signal produced by the proposed audio cryptosystem with RC6 and AES is deciphered using the proposed audio cryptosystem with RC6 and AES, and the decryption results are depicted in Fig. 5d and e. Figure 6 shows the Handel plain-audio spectrogram, Handel decipher-audio spectrogram using AES and RC6, and Handel decipher-audio spectrogram using the proposed audio cryptosystem with AES and RC6.

In order to evaluate the perceptual quality of the decipher-audio, two metrics are utilized for quality evaluation of decipher-audio signal; the SD and the correlation coefficient of the decipher-audio signal with the plain-audio signal. With increased correlation coefficient and decreased SD values, the proposed audio cryptosystem will be superior. The estimated SD and correlation coefficient values are given in Table 4. The achieved outcomes guaranteed the superiority of the proposed audio cryptosystem.

Table 3 Quality Metrics Estimations of the proposed audio cryptosystem with AES and RC6 for two cipher-audio signals encrypted with the same key and two different selected images

Quality metrics	Proposed audio cryptosystem with AES	Proposed audio cryptosystem with RC6
NPCR	99.7649	99.4549
UACI	28.0821	27.2564
r_{ab}	0.0163	0.0186
SD	Inf	Inf



(a)

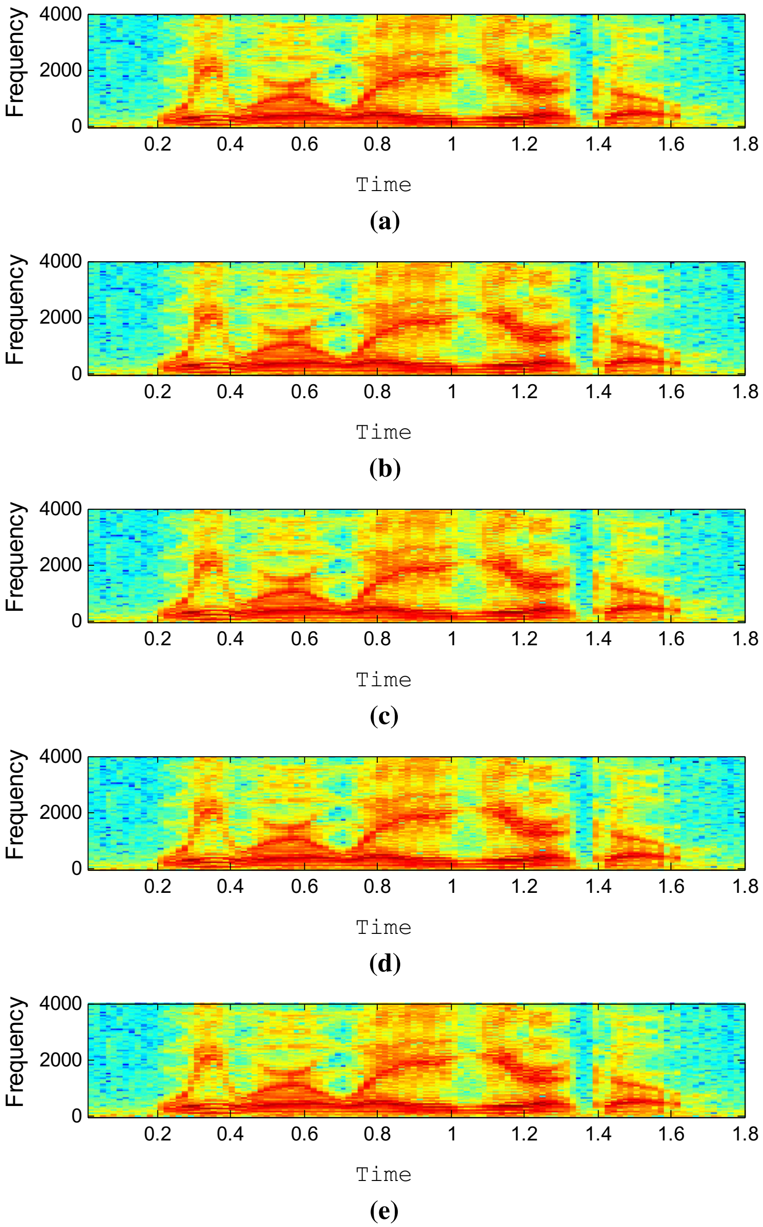
(b)

(c)

(d)

(e)

Fig. 5 Decryption results of Handel plain-audio signal. **a** Original Handel plain-audio signal. **b** Handel decipher-audio signal using AES. **c** Handel decipher-audio signal using RC6. **d** Handel decipher-audio signal using the proposed audio cryptosystem with AES. **e** Handel decipher-audio signal using the proposed audio cryptosystem with RC6



(a)

(b)

(c)

(d)

(e)

Fig. 6 Spectrogram results of decrypted Handel plain-audio signal. **a** Original Handel plain-audio signal spectrogram. **b** Handel decipher-audio signal spectrogram using AES. **c** Handel decipher-audio signal spectrogram using RC6. **d** Handel decipher-audio signal spectrogram using the proposed audio cryptosystem with AES. **e** Handel decipher-audio signal spectrogram using the proposed audio cryptosystem with RC6

Also, it can be concluded from results shown in Figs. 5, 6 and Table 4 that LSB watermarking of selected hash value with the mixed plain-audio signal prior to ciphering which may modify some bits of plain-audio signal. But, it cannot influence or damage the

Table 4 The SD and correlation coefficient estimations of the decipher-audio and plain-audio signals using the proposed audio cryptosystem with AES and RC6

Quality metrics	AES	RC6	Proposed audio cryptosystem with AES	Proposed audio cryptosystem with RC6
SD	0	0	0.4520	0.4905
Correlation coefficient	1	1	0.9997	0.9994

quality of the deciphered-audio and the decrypted cipher-audio has a good quality and high correlation with respect to the original plain-audio.

5 Conclusion

This paper presented an efficient secure audio communication system to safeguard audio information. This scheme depends on LSB watermarking and encryption. The experimental investigation ensured the immunity of the proposed scheme versus brute-force, differential and statistical attacks. The proposed scheme presents straightforward LSB authentication technique that improves the security of AES and RC6 ciphers. A private image database is utilized to enhance data security and realize authentication. Simulation tests ensured that the proposed secure audio communication system does not influence the quality of decrypted cipher-audio signal.

References

1. Li, H., Qin, Z., Shao, L., & Wang, B. (2009). A novel audio scrambling algorithm in variable dimension space. In *11th International Conference on Advanced Communication Technology ICACT 2009* (Vol. 03, pp. 1647–1651), February 15–18, 2009.
2. Anas, N. M., Rahman, Z., Shafii, A., Rahman, M. N. A., & Amin, Z. A. M. (2005). Secure speech communication over public switched telephone network. In *APACE 2005. Asia-Pacific Conference on Applied Electromagnetcs,* December 20–21, 2005.
3. Daemen, J., & Rijmen, V. (2001). Advanced Encryption Standard (AES), FIPS 197, Technical Report, Katholijke Universiteit, Leuven/ESAT, November 2001.
4. Daemen, J., & Rijmen, V. (2001). The advanced encryption standard. *Dr. Dobb's Journal, 26*(3), 137–139.
5. Lan, L. (2011). The AES encryption and decryption realization based on FPGA. In *Seventh International Conference on Computational Intelligence and Security (CIS)* (pp. 603–607).
6. Dalmisli, K. V., & Ors, B. (2009). Design of new tiny circuits for AES encryption algorithm. In *3rd International Conference on Signals, Circuits and Systems (SCS)* (pp. 1–5).
7. Feldhofer, M., Wolkerstorfer, J., & Rijmen, V. (2005). AES implementation on a grain of sand. *IEE Proceedings of Information Security, 152*(1), 13–20.
8. Lu, C., & Tseng, S. (2002). Integrated design of AES (advanced encryption standard) encrypter and decrypter. In *Proceedings of The IEEE International Conference on Application-Specific Systems, Architectures and Processors* (pp. 277–285).
9. Zhu, Q., Li, L., Liu, J., & Xu, N. (2009). The analysis and design of accounting information security system based on AES algorithm. In *International Conference on Machine Learning and Cybernetics* (Vol. 5, pp. 2713–2718).
10. Rivest, R. L., Robshaw, M. J. B., Sidney, R., & Yin, Y. L. (1998). *The RC6TM block cipher*. Cambridge, MA: M. I. T Laboratory for Computer Science.

11. Contini, S., Rivest, R. L., Robshaw, M. J. B., & Yin, Y. L. (1998). The Security of the RC6TM Block Cipher (Version 1.0). RSA Laboratories, M. I. T Laboratory for Computer Science.
12. Ragab, A. H. M., Ismail, N. A., & FaragAllah,O. S. (2001). Enhancements and implementation of RC6 block cipher for data security. In *Proceedings of International Conference on Electrical and Electronic Technology* (Vol. 1, pp. 133–137).
13. Meier, W., Knudsen, L. R. (2000). Correlations in RC6 with a reduced number of rounds source. In *Proceedings of The 7th International Workshop on Fast Software Encryption* (pp. 94–108).
14. Kim, G., Kim, J., & Cho, G. (2009). An improved RC6 algorithm with the same structure of encryption and decryption. In *The 11th International Conference on Advanced Communication Technology (ICACT)* (Vol. 2, pp. 1211–1215).
15. Den Boer, B., & Bosselaers, A. (1994). Collisions for the compression function of MD5. In T. Helleseth (Ed.), *Advances in Cryptology. proc. Encrypt′ 93. LNCS 765* (pp. 293–304). Springer.
16. Dobbertin, H. (1996). The status of MD5 after a recent attack, RSA laboratories. *CryptoBytes*, *2*(2), 1–6.
17. Elshamy, E. M., El-Rabaie, S., Faragallah, O. S., Elshakankiry, O., Abd El-Samie, F. E., El-sayed, H. S., et al. (2015). Efficient audio cryptosystem based on chaotic maps and double random phase encoding. *International Journal of Speech Technology, 18*(4), 619–631.
18. Elhoseny, H. M., Faragallah, O. S., Ahmed, H. E. H., Kazemian, H. B., El-sayed, H. S., & Abd El-Samie, F. E. (2016). The effect of fractional Fourier transform in encryption quality for digital images. *Optik-International Journal for Light and Electron Optics, 127*(1), 315–319.
19. Elhoseny, H. M., Ahmed, H. E. H., Abbas, A. M., Kazemian, H. B., Faragallah, O. S., El-Rabaie, S. M., et al. (2015). Chaotic encryption of images in the fractional Fourier transform domain using different modes of operation. *Signal, Image and Video Processing Journal, 9*(3), 611–622.
20. Elshamy, A. M., Rashed, A. N. Z., Mohamed, A. E. N. A., Faragallah, O. S., Mu, Y., Alshebeili, S. A., & El-Samie, F. A. (2013). Optical image encryption based on chaotic baker map and double random Phase encoding. *IEEE/OSA Journal of Lightwave Technology*, *31*(15), 2533–2539.
21. Hedelin, P., Norden, F., & Skoglund, J. (1999). SD optimization of spectral coders. In *IEEE Workshop on Speech Coding Proc.* (pp. 28–30).
22. Faragallah, O. S., & Afifi, A. (2017). Optical color image cryptosystem using chaotic baker mapping based-double random phase encoding. *Optical and Quantum Electronics*, *49*(3), 1–28.
23. Elashry, I. F., Faragallah, O. S., Abbas, A. M., El-Rabaie, S., & Abd El-Samie, F. E. (2009). Homomorphic image encryption. *Journal of Electronic Imaging, 18*(3), 033002.

Osama S. Faragallah received the B.Sc. (Hons.), M.Sc., and Ph.D. degrees in Computer Science and Engineering from Menoufia University, Menouf, Egypt, in 1997, 2002, and 2007, respectively. He is currently Associate Professor with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University, where he was a Demonstrator from 1997 to 2002 and has been Assistant Lecturer from 2002 to 2007 and since 2007 he has been a Teaching Staff Member with the Department of Computer Science and Engineering, Faculty of Electronic Engineering, Menoufia University. He is a coauthor of about 100 papers in international journals and conference proceedings, and two textbooks. His current research interests include network security, cryptography, internet security, multimedia security, image encryption, watermarking, steganography, data hiding, medical image processing, and chaos theory.